ITS
Office of Information Technology Services

Security Assessment Project

Vendor Training

October 8, 2003

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Project Background - Security Legislation

- Compliance with Section 1.(a) G.S. 147-33.82, Section 1.(a) is amended by adding a new section to read:"(e1) The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. Not later than May 4, 2004, the Information Resources Management Commission and the State Chief Information Officer shall submit a public report that summarizes the status of the assessment, including the available estimates of additional funding needed to bring agencies into compliance, to the Joint Legislative Commission on Governmental Operations and shall provide updated assessment information by January 15 of each subsequent year."

Project Background - Security Legislation

- The State CIO shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established
- The assessment shall include, at a minimum,
  - the rate of compliance with the standards in each agency
  - an assessment of each agency's security organization, network security architecture
  - current expenditures for information technology security.
  - cost to implement the security measures needed for agencies to fully comply with the standards.
- Each agency subject to the standards shall submit information required by the State CIO for purposes of this assessment.
- Not later than May 4, 2004, the IRMC and the State CIO shall submit a public report to the Joint Legislative Commission on Governmental Operations, that
  - summarizes the status of the assessment
  - includes estimates of additional funding needed to bring agencies into compliance
- The IRMC and State CIO shall provide updated assessment information by January 15 of each subsequent year.

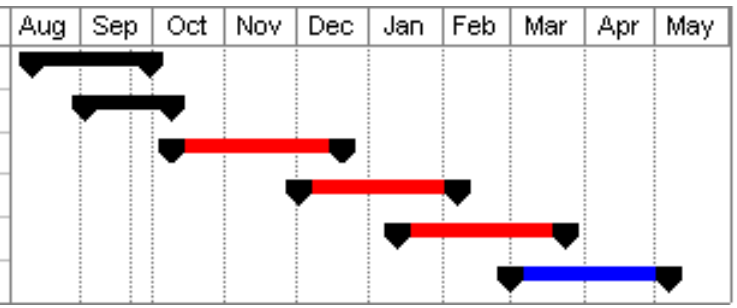
Office of Information Technology Services

Project Background - Timeline

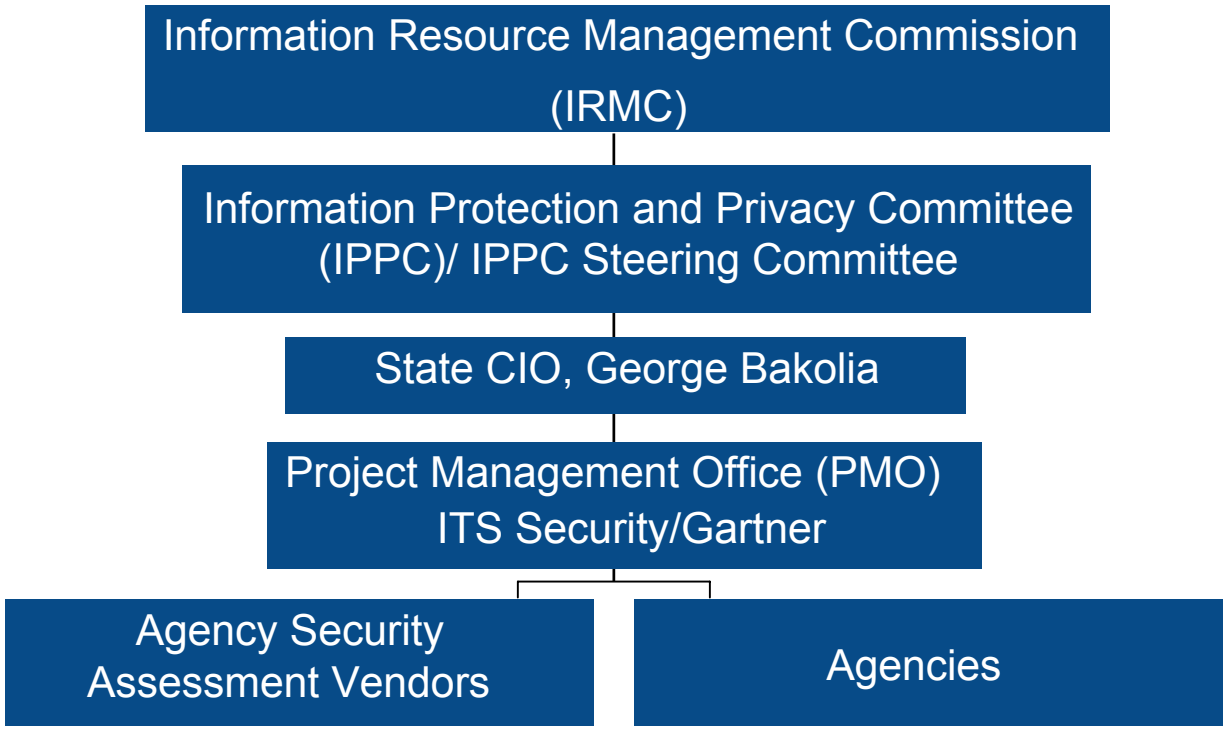
- Security assessment project is 4-phase process.
- Phases 1 and 2 consist of preparation by the Project Management Office (PMO)
- Phase 3: Security assessments will be conducted in 3 Groups:
  - Group 1 - October 13 – December 4
  - Group 2 - December 2 – February 3
  - Group 3A - January 12 – March 24
  - Group 3B - January 28 – March 24

  PMO prepares preliminary findings and extrapolated estimates beginning Dec.
- Phase 4 - PMO identifies statewide security risks and develops cost and resource estimate for statewide corrective action.

ID	Task Name
1	**Phase 1 - Organize Project Management Office**
2	**Phase 2 - Assessment Preparation**
3	**Phase 3 - Conduct Security Assessments (Group 1)**
4	**Phase 3 - Conduct Security Assessments (Group 2)**
5	**Phase 3 - Conduct Security Assessments (Group 3)**
6	**Phase 4 - Develop Final Report**



Security Project Reporting Structure



Office of Information Technology Services

Project Responsibilities

Participants	Primary Responsibilities
Project Management Office – ITS / Gartner	• Develop all project tools and templates • Manage assessment project • Develop preliminary and extrapolated cost estimates • Develop final recommendations and final cost estimates • Train vendors in use of tools and templates • Project reporting
Vendors	• Conduct assessments of assigned agencies • Project Management/Reporting to PMO (status, issues, etc.)
Agencies	• Led by agency security liaison • Prepare for assessments • Provide documentation • Participate in assessments

Project Team Introductions

- **ITS Team Members**
  - Ann Garrett, Project Sponsor
  - Charles “Chip” Moore, Security Analyst
  - Julean Self, Planning Analyst
  - Christopher “Chris” Turpin, Security Analyst
- **Gartner Team Members**
  - John Dubiel, Subject Matter Expert
  - Daniel Saroff, Subject Matter Expert
  - Elizabeth Sernoff, Project Team Member
  - Ruth Steinberg, Engagement Manager
  - Lance Westerlund, Project Manager

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Vendor Compliance with State Policies

- All vendor staff must have completed NDAs and background checks on-file with the PMO
- Vendors must protect the confidentiality of agency data and assessment results
- Vendors are responsible for the proper disposition of all State materials upon completion of the project
  - Vendor cannot retain any State information
- Vendors must protect the intellectual property of other vendors
- All questions, concerns and issues must be directed to the PMO
- Failure to abide by the State's Policies may result in contract termination

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Security Assessment Project Overview

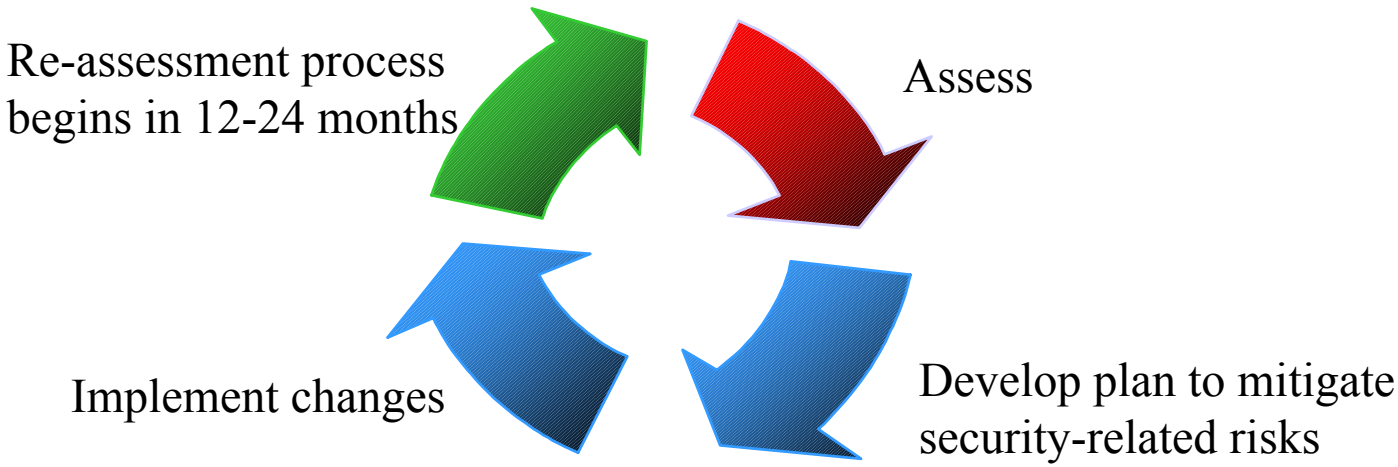
- Project Background
- Approach and Methodology
- Vendor Responsibilities
- Deliverables
- Critical Success Factors

Project Background - Response

- In response to provisions North Carolina Session Law 2003-153, which states that periodic agency security assessments will be performed by the State Chief Information Officer (SCIO), the State of North Carolina has initiated a statewide security assessment of all Executive Branch agencies.
- Assessment process is intended to provide key-decision makers with:
  - Global view of the security status of agencies
  - Detailed findings sufficient to permit State to prioritize and budget for required remediation efforts.
- Assessment will be based on the North Carolina Security Policy which is based on ISO17799 standard.

Assessment Process Definition

- A process of defining, selecting, designing, collecting, analyzing, interpreting, and using information for the purpose of determining how well performance matches baseline standards and expectations.



Approach & Methodology

- There are four ways to capture security information. The State's Security Assessment Project will use the first two.

Policy standard and guidelines review – Assessment team conducts a paper review

"Eyes-on" security review– Reconciliation of security policies v. deployment; typically involves spot checking of key systems to verify compliance

"Hands-on" security review – Detailed audit of asset configuration

Vulnerability assessment– Series of sanctioned attacks designed to probe system

Office of Information Technology Services

Approach & Methodology - Assessment Focus Areas

The assessment methodology leverages the ISO 17799 framework.

Security Policy	Management support, commitment, direction in accomplishing information security goals
Organizational Security	Need for management framework that creates, sustains, and manages security infrastructure of organization
Asset Classification and Control	Ability of security infrastructure to protect organizational assets
Personnel Security	Organization's ability to mitigate risk inherent in human interactions
Physical Security	Risk inherent to organizational premises
Communications & Operations	Organization's ability to ensure correct and secure operation of its assets

Approach & Methodology -
Assessment Focus Areas (Cont.)

Access Administration	Organization's ability to administratively control access to assets based on business and security requirements
Access Technology	Organization's ability to control access to technology-specific assets based on business and security requirements
Applications Development & Maintenance	Organization's ability to ensure appropriate information system security controls are incorporated and maintained
Business Impact / Continuity	Organization's ability to counteract interruptions to normal operations
Compliance	Organization's ability to remain in compliance with regulatory, statutory, contractual and security requirements.

Office of Information Technology Services

Approach & Methodology -
Scope of the Assessment

Security Assessment Scope Overview											
	100: Info Security Project Charter	**110:** Security Policy	**120:** Organizational Security	**130:** Asset ID & Classification	**140:** Personnel Security	**150:** Physical & Enviro Security	**160:** Comms & Ops Management	**170:** Access Control	**180:** Systems Dev & Maintenance	**190:** Business Continuity Mgmt	**200:** Compliance
People											
Agency / IT Management	◆	◆	◆		◆	◆	◆			◆	◆
Insourced	◆	◆	◆		◆	◆	◆			◆	◆
Outsourced Services (e.g. off site)	◆	◆	◆		◆	◆	◆			◆	◆
Out-tasked Services (e.g. on site)	◆	◆	◆		◆	◆	◆			◆	◆
Hardware											
Mainframe		◆		◆		◆		◆	◆	◆	◆
Midrange		◆		◆		◆		◆	◆	◆	◆
NAS / SAN		◆		◆		◆		◆	◆	◆	◆
Desktops		◆		◆		◆		◆	◆	◆	◆
Laptops		◆		◆		◆		◆	◆	◆	◆

Excerpt from the Scope section of the Requirements Document.

Duration of Assessment

- Vendors must tailor their assessment activities to fit the available time and budget constraints.

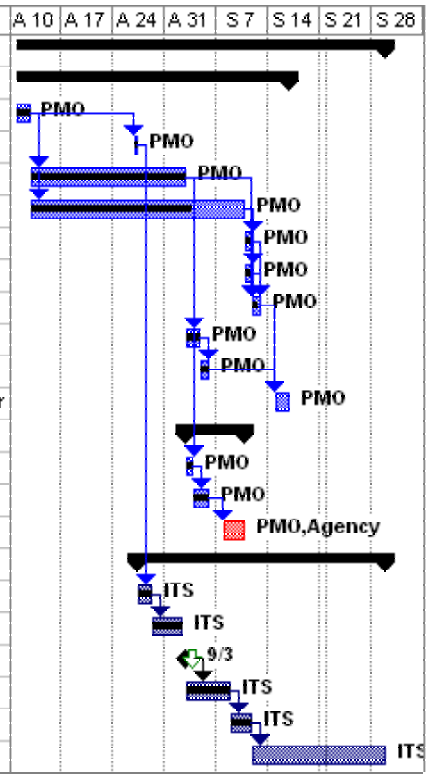
	Type 1	Type 2	Type 3
Number of Agencies	11	11	3
Fact Finding/Diligence Effort	2 weeks	2.5 weeks	3 weeks
Findings Development	1 week	1.5 weeks	2 weeks
Total Time to Complete Assessment *	3 weeks	4 weeks	5 weeks
Hours Cap (per agency)	200	300	400
Note: all times are stated in calendar weeks except Hours Cap			
* Does not include planning and agency debrief activities			

Phase 1. Organize PMO

Phase 1 was largely transparent to agencies and vendors and included the following tasks:

- Step 1. Prepare Tools and Processes
- Step 2. Prepare Agency Assessment Schedule
- Step 3. Vendor Selection

ID	Task Name
1	**Phase 1 - Organize Project Management Office**
2	**Step 1 - Prepare Tools and Processes**
3	1.1.1 - Prepare Kick-off Meeting Materials
4	1.1.2 - Project KOM
5	1.2 - Prepare Requirements
6	1.3 - Prepare Security Assessment Tool
7	1.4 - Develop Assessment Scorecard
8	1.5 - Develop Vendor Progress Report Templates
9	1.6 - Develop Project Progress Report Template
10	1.7.1 - Develop Assessment Cost Estimates
11	1.7.2 - Finalize Cost Estimates with State
12	1.8 - Develop Deliverable Review and Acceptance Forr
13	**Step 2 - Prepare Agency Assessment Schedule**
14	2.1 - Develop Agency Prioritization Tool
15	2.2 - Perform Prioritization Analysis
16	2.3 - Validate Assessment Schedule with Agencies
17	**Step 3 - Vendor Selection**
18	3.1 - Prepare Vendor Requirements
19	3.2 - Develop Evaluation Criteria and Tools
20	3.3 - Vendor Responses Due
21	3.4.1 - Evaluate Vendor Responses
22	3.4.2 - Vendor Selection Determination
23	3.4.3 - Vendor Approval and Contracting

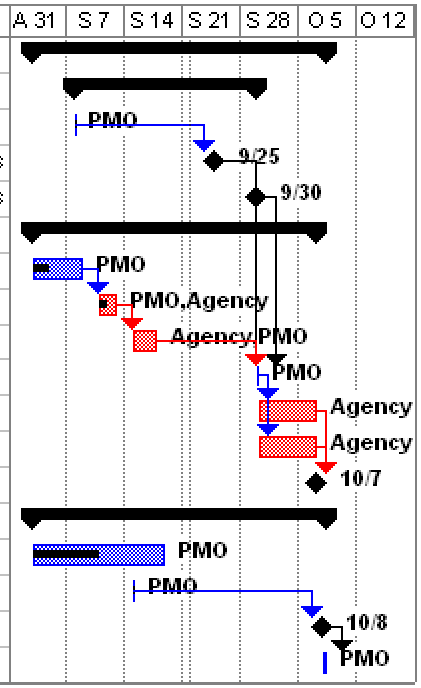


Phase 2. Assessment Preparation

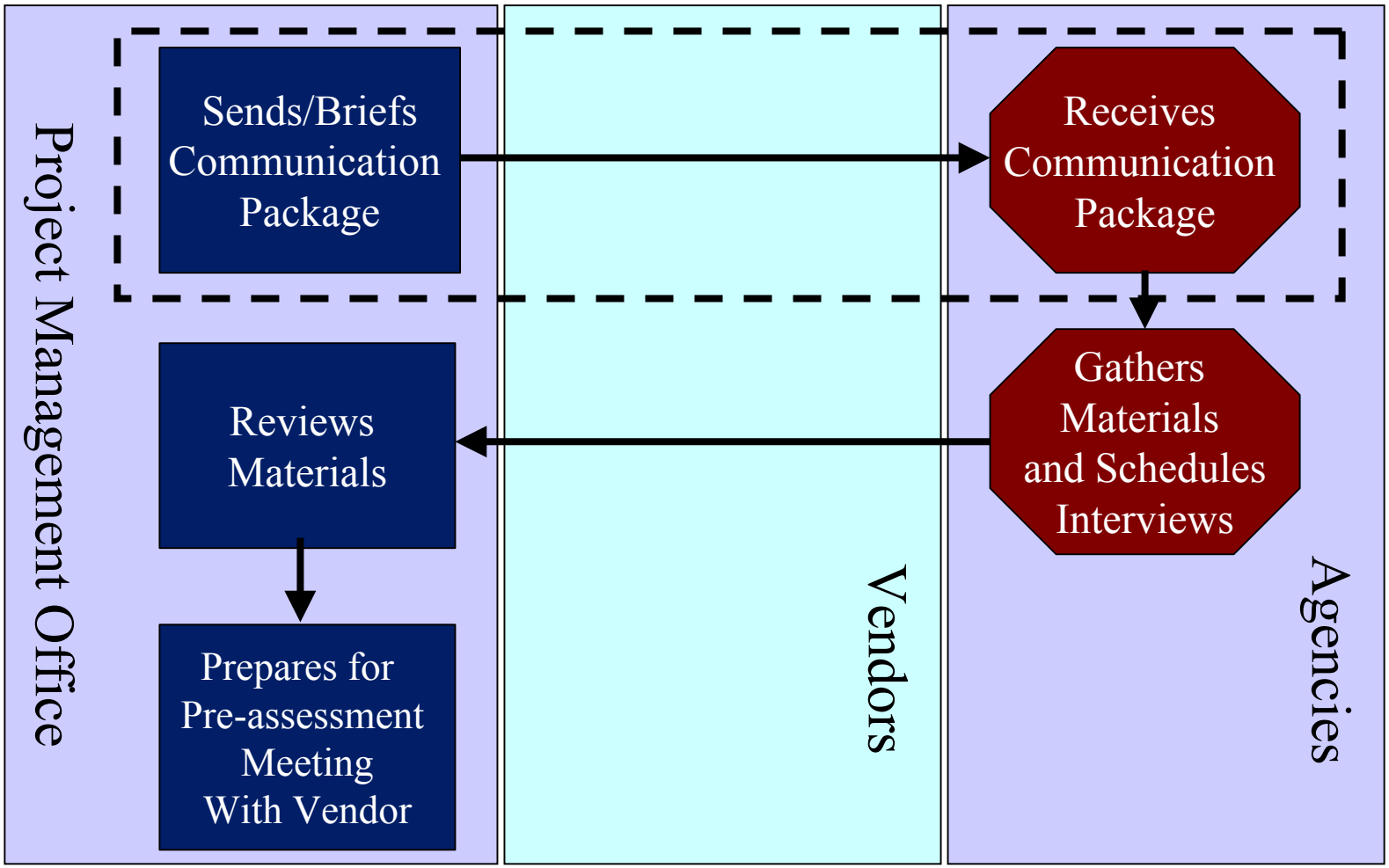
Phase 2 was designed to get agencies and vendors aligned and up-to-speed. It includes:

- Step 4. Preliminary Agency Coordination
- Step 5. Agency Preparation
- Step 6. Vendor Preparation - Training

ID	Task Name
24	**Phase 2 - Assessment Preparation**
25	**Step 4 - Preliminary Agency Coordination**
26	4.1 - Invite Key Stakeholders to Overview Meeting
27	4.2 - Conduct Agency Project Overview Meeting (Sess
28	4.2 - Conduct Agency Project Overview Meeting (Sess
29	**Step 5. Agency Preparation**
30	5.1 - Develop Resource Requirement Guidelines
31	5.2 - Identify Specific Resources at State Agencies
32	5.3 - Coordinate Assessment Start Date
33	5.4 - Provide Agency with Communications Package
34	5.5 - Collect Background Information
35	5.6 - Schedule Agency Interviews
36	5.7 - Agency Preparation Due Date
37	**Step 6. Vendor Preparation - Training**
38	6.1 - Develop Training Materials
39	6.2 - Set Training Session Date
40	6.3 - Conduct Training Session
41	6.4 - Provide Vendors with State Policies

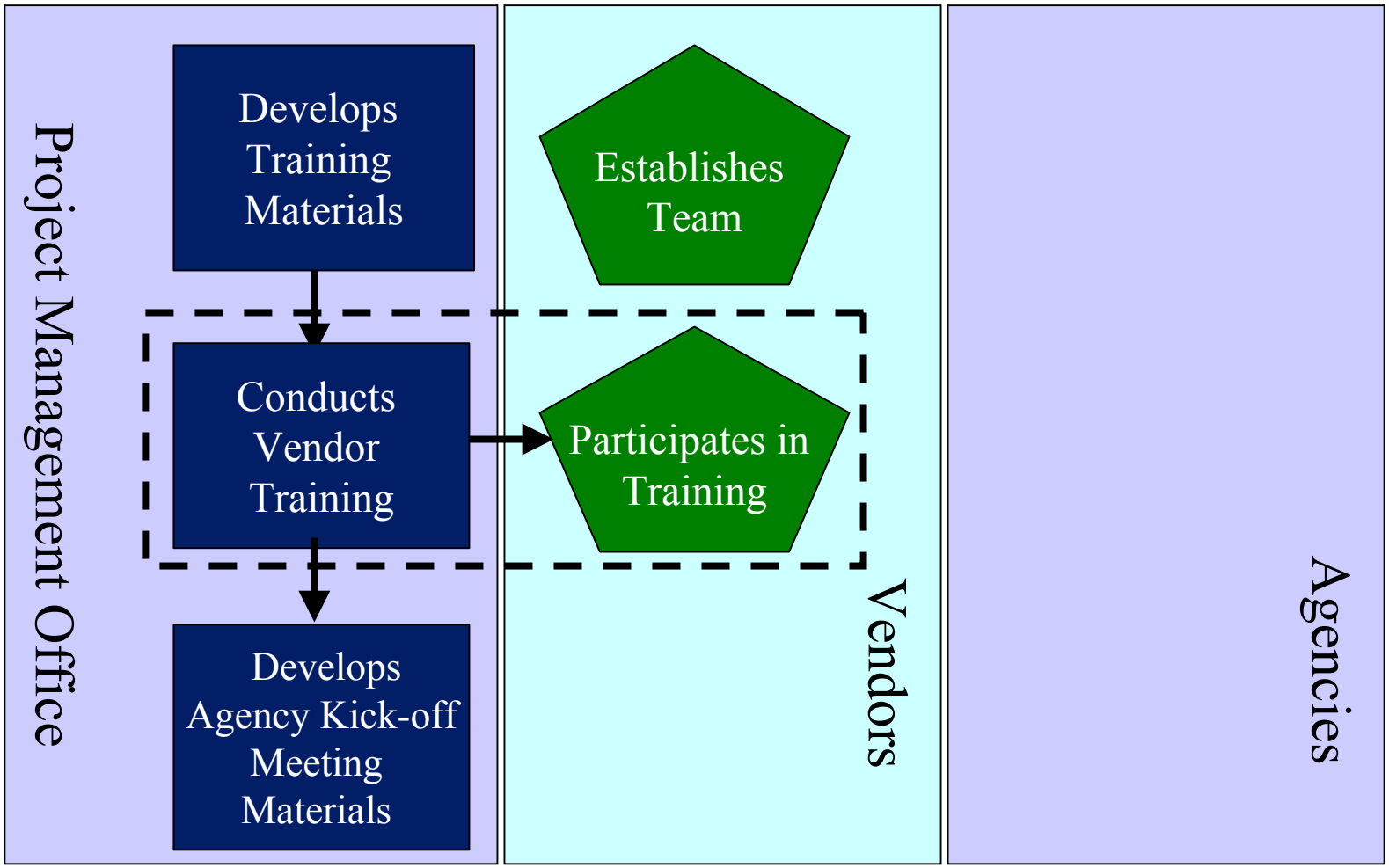


Step 5: Agency Preparation



Office of Information Technology Services

Step 6: Vendor Preparation



Types of Agency Data

- Five (5) business days prior to scheduled assessment kick-off date, Agency delivers the following types of information to the PMO:
  - Contact Information List of staff members to be interviewed with a proposed interview schedule
  - Checklist of documentation for review by vendors
- Intent is to familiarize vendor with agency's organizational structure, security policies and procedures, etc.
- Once vendor is on site, additional information is collected during meetings, interviews, etc.
- Specific guidance as to what documentation is required is contained in Agency Preparation Communications Package.

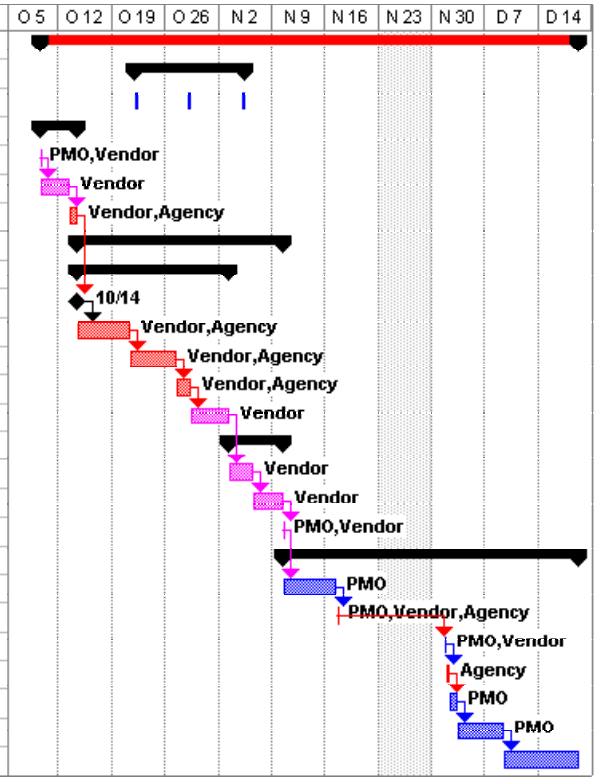
Office of Information Technology Services

Phase 3. Conduct Security Assessments

Phase 3 covers the actual assessment and report generation process. It includes:

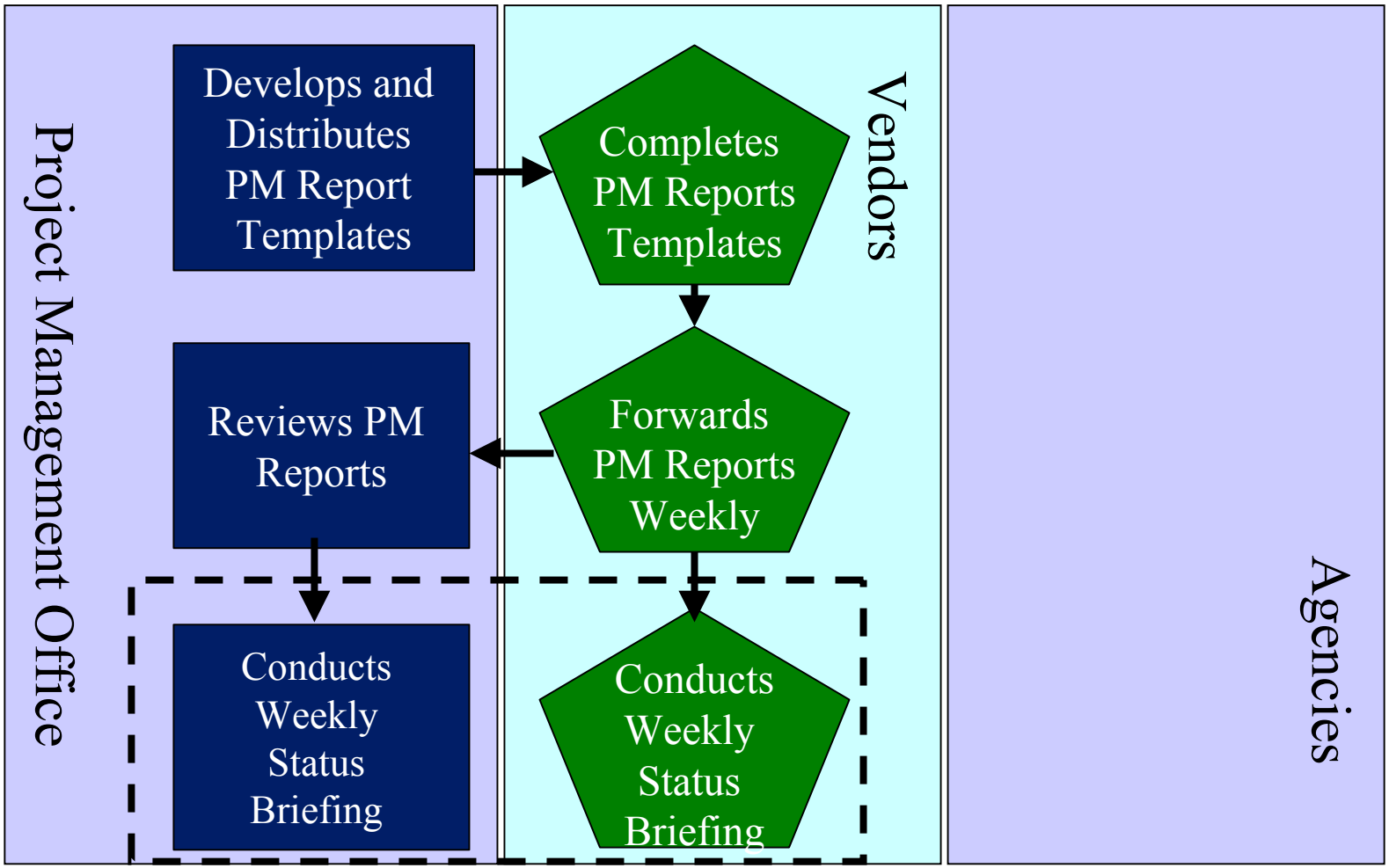
- Step 7. Project Status Reporting
- Step 8. Prepare for Agency Assessment
- Step 9. Conduct Agency Assessment
- Step 10. Assessment Closeout

ID	Task Name
42	**Phase 3 - Conduct Security Assessments (Group 1)**
43	**Step 7 - Project Status Reporting**
44	**7.1 - Weekly Update Reports and PMO Briefings**
48	**Step 8 - Prepare for Agency Assessment**
49	8.1 - Conduct Pre-Assessment Meeting
50	8.2 - Review Agency Materials
51	8.3 - Finalize Interview Schedule and Plan
52	**Step 9 - Conduct Agency Assessment**
53	**Task 9.1 - Collect Information**
54	9.1.1 - Conduct Assessment Kickoff Meeting
55	9.1.2 - Conduct Assessment Interviews
56	9.1.3 - Collect and Review Documentation
57	9.1.4 - Conduct Compliance Review
58	9.1.5 - Develop Preliminary Findings
59	**Task 9.2 - Analyze Data and Prepare Reports**
60	9.2.1 - Complete Assessment Documentation
61	9.2.2 - Develop Findings Summary
62	9.2.3 - Conduct PMO Debrief
63	**Step 10 - Assessment Closeout**
64	10.1 - Review and Accept Deliverables
65	10.2 - Schedule Agency Debrief
66	10.3 - Conduct Agency Debrief
67	10.4 - Complete Vendor Evaluation Form
68	10.5 - Update Project Records and Close Project
69	10.6 - Extract Data for Final Report
70	10.7 - Develop Preliminary Statewide Findings Report



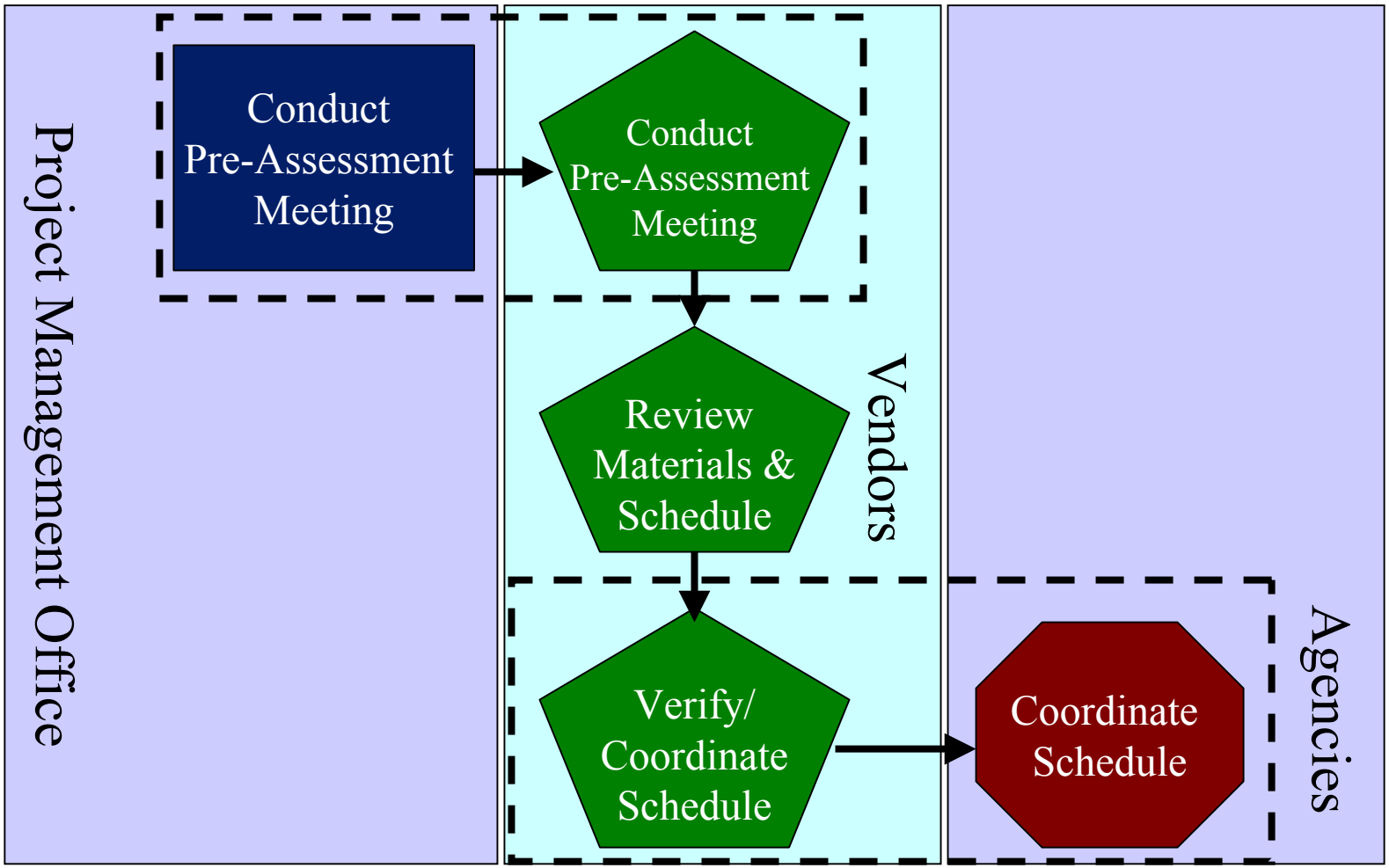
Office of Information Technology Services

Step 7: Project Status Reporting



Office of Information Technology Services

Step 8: Prepare for Agency Assessment



Step 9 Task 1: Conduct Agency Assessments

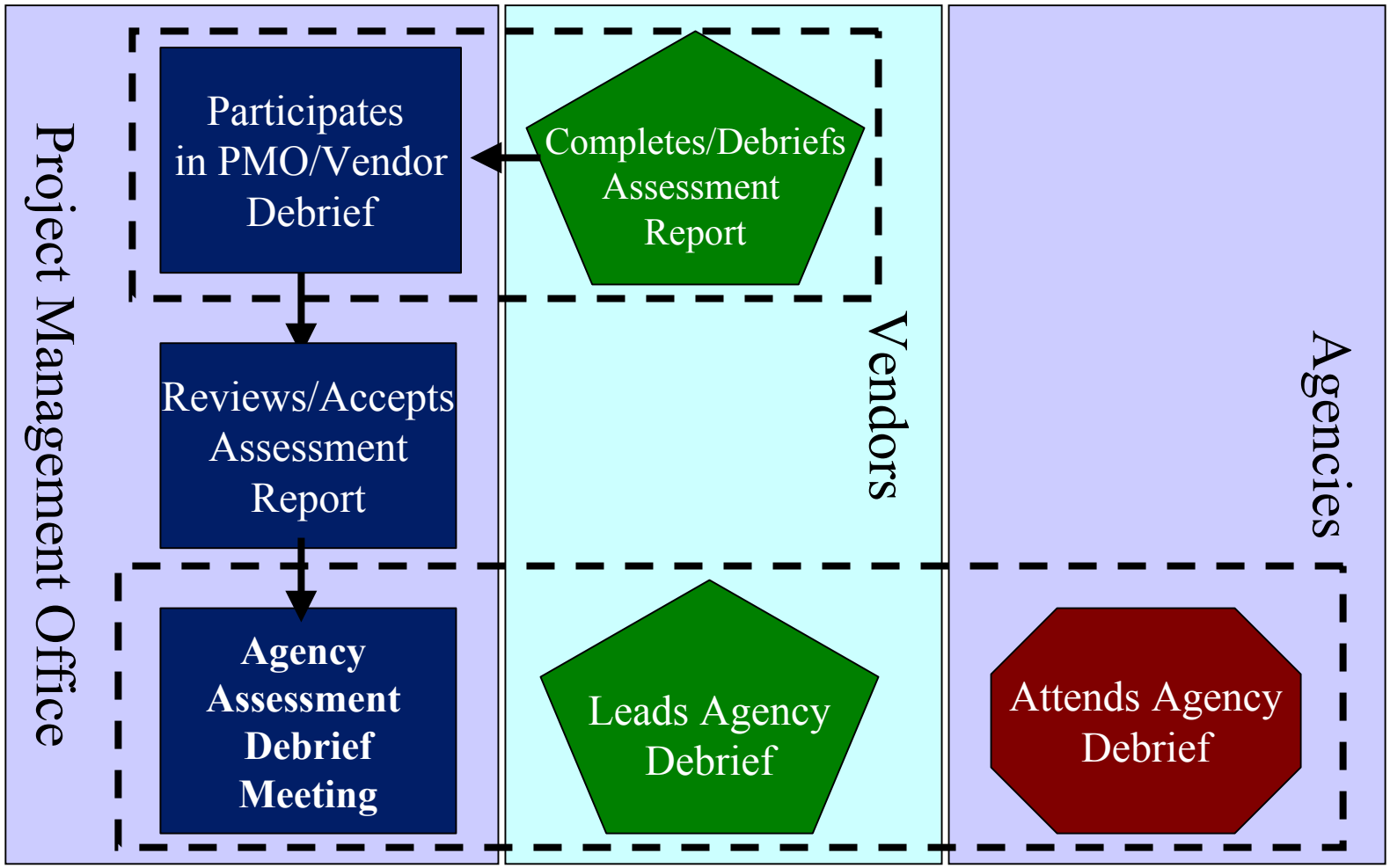
- Conduct Agency Assessment Kick-off Meeting
- Conduct Interviews with Key Personnel
- Review Documentation in Support of Policies
- Conduct Spot-checks/Observations at the Agency

Interview Guidelines

- Agencies have been asked to arrange interviews with the following types of staff:
  - IT Management
  - Agency security liaison
  - Physical security team
  - Networking / Operations staff
  - Human resources and/or individual(s) responsible for employee background checks
  - Business Continuity Manager / Lead
  - Other technical resources, as appropriate
- Same staff would normally attend vendor kickoff and agency debrief meetings.

Office of Information Technology Services

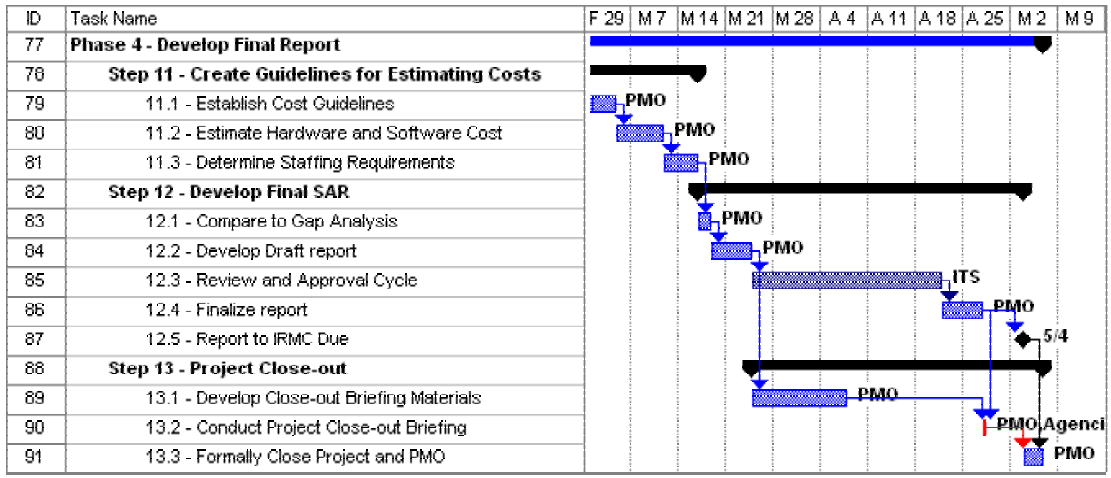
Step 9 Task 2 and Step 10: Assessment Closeout



Phase 4. Develop Final Report

Phase 4 is largely transparent to Agencies and Vendors and covers the final report generation process. It includes:

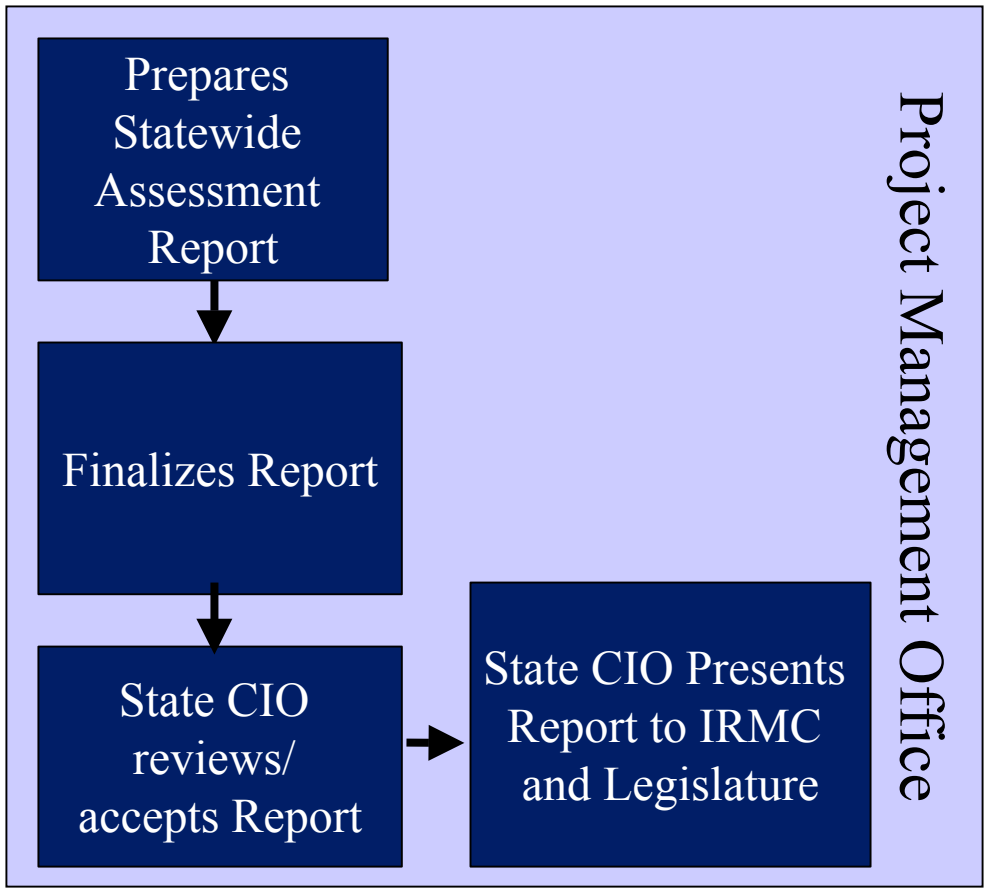
- Step 11. Create Guidelines for Estimating Cost
- Step 12. Develop Final Security Assessment Report (SAR)
- Step 13. Project Closeout



ID	Task Name
77	**Phase 4 - Develop Final Report**
78	**Step 11 - Create Guidelines for Estimating Costs**
79	11.1 - Establish Cost Guidelines
80	11.2 - Estimate Hardware and Software Cost
81	11.3 - Determine Staffing Requirements
82	**Step 12 - Develop Final SAR**
83	12.1 - Compare to Gap Analysis
84	12.2 - Develop Draft report
85	12.3 - Review and Approval Cycle
86	12.4 - Finalize report
87	12.5 - Report to IRMC Due
88	**Step 13 - Project Close-out**
89	13.1 - Develop Close-out Briefing Materials
90	13.2 - Conduct Project Close-out Briefing
91	13.3 - Formally Close Project and PMO

Office of Information Technology Services

Phase 4: Develop Final Statewide Security Assessment Report



Office of Information Technology Services

Vendor Deliverables

Weekly

- Weekly Vendor Project Status Report Including:
  - Project Performance Dashboard
  - Key Findings Summary
  - Open Task Report
  - Project Issues Log
  - Agency Documentation List
  - Vendor Time Sheet

Final

- Security Assessment Findings Overview
- Completed Assessment Tool
- Final Project Status Report
- Returned Agency Documentation
- Interview Schedule (as-built)

Please Note Naming Convention: NC AgencyAbbreviation ToolName_MMDD (e.g. NC DOT PM Tools_1013)

Critical Success Factors

- Agencies dedicate adequate resources toward effort
- Vendors provide experienced, knowledgeable assessment teams that add value to the project
- All participants properly prepare for assessment
- Roles and responsibilities for all participating parties clearly understood
- All participants adhere to project schedule and budget
- Risks identified, documented and mitigated promptly and openly
- Communication remains open and honest

There are no additional resources available to allow for time or budget overruns

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Office of Information Technology Services

Security Assessment Tool Overview

- The vendor works interactively with the agencies to complete the tool
- The assessment tool is based on the ten ISO17799 categories. ISO 17799 category Access Control is sub-divided into two categories (7a,7b) for a total of 11 categories
- Each category is sub-divided into sub-sections of related questions
- Scoring of each category section provides an overall category score
- Category scores populate the Summary dashboard providing an overall Agency score

1. Security Policy	4.00

Security Assessment - Summary Score

Area of Focus	Raw Score	Weight	Adj. Score
1. Security Policy	4.00	9%	0.3636
2. Organizational Security	4.00	9%	0.3636
3. Asset Classification & Control	4.00	9%	0.3636
4. Personnel	4.00	9%	0.3636
5. Physical Security	4.00	9%	0.3636
6. Operations	4.00	9%	0.3636
7A. Access Administration	4.00	9%	0.3636
7B. Access Technology	0.00	9%	0
8. Applications	4.00	9%	0.3636
9. Business Impact - Continuity	4.00	9%	0.3636
10. Compliance	4.00	9%	0.3636
Total Score	**3.6**	**100%**	**3.6364**

1.1	Security Policies, Standards, & Procedures	Quality (1=Best Practice 2=Meets Reqs 3=Deficient 4=Unacceptable Blank = Not Applicable)	Execution (1=Fully 2=Critical Areas 3=Minimal/Gaps 4=None/WIP Blank = Not Applicable)	Justification
1.1.1	Is there an agency security PSP in place?	4	4	
1.1.2	Does the PSP state what is and is not permissible?			
1.1.3	Is the agency PSP in compliance with State Security PSPs?			
1.1.4	Have the State PSPs been augmented to reflect unique agency requirements?			
1.1.5	Does the scope of the PSP cover all facets of information?			
1.1.6	Does the PSP define and identify what is classed as information?			
1.1.7	Does the PSP define and identify organizational perimeters?			
1.1.8	Does the PSP identify management and employee responsibilities?			
1.1.9	Does the PSP make clear the consequences of noncompliance?			
1.1.10	Has it been updated/reviewed in the past 12 months?			
1.1.11	Has management approved the PSP?			
1.1.12	Is there an information security PSP that covers contractors?			
1.1.13	Does the security PSP assign responsibility and do the job description(s) reflect this responsibility?			

Office of Information Technology Services

Security Assessment Tool Overview

- Category Full Title
- Section Title
- Section Questions
- Quality Score
  - Completeness of agency Policies, Standards and Procedures (PSP)
- Execution Score
  - Application of agency PSP to systems and services
- Justification
  - Brief statement explaining all scores

3. Asset Classification and Control

3.1	Accountability	Quality (1=Best Practice, 2=Meets Reqs, 3=Deficient, 4=Unacceptable, Blank = Not Applicable)	Execution (1=Fully, 2=Critical Areas, 3=Minimal/Gaps, 4=None/WIP, Blank = Not Applicable)	Justification
3.1.1	Is logical access to assets fully controlled?	4	4	
3.1.2	Is the asset inventory complete (dB, software, hardware, services)?			
3.1.3	Is there an audit log to identify the individual and the time of access for nonstandard hours of access?			
3.1.4	Are procedures in place for the proper disposal of confidential information?			
	Average	**4.00**	**4.00**	

Vendor Category Score- Accountability		

Total Score	**4.00**	**4.00**	(average)

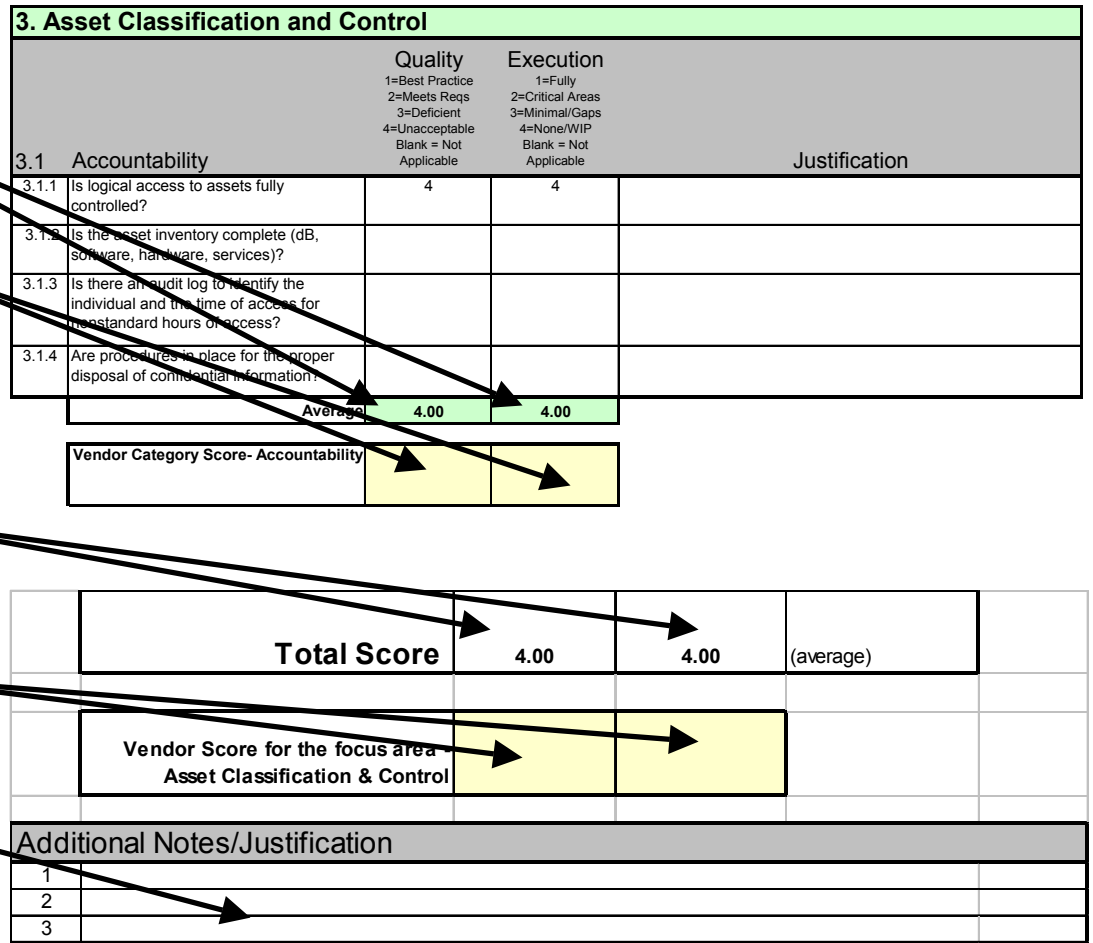
Vendor Score for the focus area - Asset Classification & Control		

Additional Notes/Justification	
1	
2	
3	

Office of Information Technology Services

Security Assessment Tool Overview

- Averaged Section Score
  - Calculated score
- Vendor Assigned Score
  - May be different from the calculated scores. Difference is based on relevance to Agency security requirements
- Total Category Score
  - Calculated score for section
- Vendor Assigned Total Category Score
- Free Form Comment Field
  - Information supporting vendor assigned scores, etc.



3. Asset Classification and Control				
3.1	Accountability	Quality (1=Best Practice, 2=Meets Reqs, 3=Deficient, 4=Unacceptable, Blank = Not Applicable)	Execution (1=Fully, 2=Critical Areas, 3=Minimal/Gaps, 4=None/WIP, Blank = Not Applicable)	Justification
3.1.1	Is logical access to assets fully controlled?	4	4	
3.1.2	Is the asset inventory complete (dB, software, hardware, services)?			
3.1.3	Is there an audit log to identify the individual and the time of access for nonstandard hours of access?			
3.1.4	Are procedures in place for the proper disposal of confidential information?			
	Average	4.00	4.00	
	Vendor Category Score- Accountability			
	Total Score	4.00	4.00	(average)
	Vendor Score for the focus area - Asset Classification & Control			

Additional Notes/Justification
1
2
3

Scoring Guidelines

- Scoring is on a 1 to 4 scale
  - 1 is the best score; 4 is the worst score.
  - All questions must be scored.
  - If a vendor thinks that a question not applicable to a specific agency, score must be left blank. The notation "N/A" and a complete justification must be entered into the justification column.
  - Fully and completely justify all scores of 1 or 4
- Scoring has two key components: Quality and Execution
  - Score Quality first, then Execution

The lower the number, the better the security.
Number 1 is best!

Scoring Guidelines (Cont.)

- **Quality** represents whether the agency has addressed the security question in an effective and complete fashion in its Policies, Standards and Procedures (PSP). Its scoring criteria are:
  - **1. Best Practice:** The agency thoroughly addresses all present requirements and PSPs are designed to be flexible and robust enough to cover any requirements. Agency PSP requires controls and security techniques that exceed "standard industry practice" and reflect the approaches being employed at leading firms.
  - **2. Meets Requirements:** The agency addresses present security requirements. Policies, Standards and Procedures are commensurate with those recognized as "standard industry practice" but do not necessarily reflect the latest best practices.
  - **3. Deficient:** The means used to address the security requirement do not meet standard industry practice and are not adequate for the agency's requirement.
  - **4. Does Not Meet Requirements:** The agency does not address the security requirement or does so so inadequately as to prove impractical or ineffective.

Scoring Guidelines (Cont.)

- **Execution** represents whether the agency has deployed security PSP in an encompassing fashion. Its scoring criteria are:
  - **1. Fully:** All relevant security areas are addressed. PSP are applied across all applicable and allied systems, technologies, platforms, etc.
  - **2. Critical Areas:** Critical and some ancillary systems/technologies are addressed or are in compliance with agency PSP requirements.
  - **3. Gaps:** Critical and ancillary systems are partially covered or are in partial compliance with agency PSP requirements. Significant disparity exists between the applicable standard and current provisions as deployed.
  - **4. None/Work in Progress (WIP):** Agency has not addressed the security requirements or is in process of developing a method to address requirement.

Office of Information Technology Services

Scoring Guidelines - Example 1

- Quality Scoring
  - –Question: Are procedures in place for the proper disposal of confidential information?
  - –Response Details:
    - **Quality Score of:**

1 - Best Practice: Confidentiality is clearly defined with differing disposal requirements based on information type for all systems. Existing documentation is covered and categorized. Policy is flexible enough to address any requirements defined by State and Federal agencies.

2 - Meets Requirements: Confidentiality is defined for current Agency requirements. Existing documentation confidentiality requirements are defined and adequately address State's and Federal confidentiality requirements.

3 - Deficient: Confidentiality is incompletely defined. Only critical types of documentation are covered. Disposal requirements are poorly defined. Limited document categorization.

4 - Does Not Meet Requirements: Confidentiality is not defined. No identification of documents or types covered by the confidentiality. Poor disposal mechanisms.

3.1	Accountability	Quality 1=Best Practice 2=Meets Reqs 3=Deficient 4=Does Not Meet Reqs Blank = Not Applicable	Execution 1=Fully 2=Critical Areas 3=Minimal/Gaps 4=None/WIP Blank = Not Applicable	Justification
3.1.4	Are procedures in place for the proper disposal of confidential information?	1		

Office of Information Technology Services

Scoring Guidelines - Example 1 (Cont.)

- Execution Scoring
  - –Question: Are procedures in place for the proper disposal of confidential information?
  - –Response Details:
    - **Execution Score of:**

1 - Fully: Confidential documents are stored in a secure facility. All confidential information is disposed of appropriately to the level required (relevant documentation is addressed by the existing PSP). The full spectrum of documentation is identified for its confidentiality.

2 - Critical Areas: Confidential documents are stored in a secure facility prior to destruction. Critical confidential information is disposed of appropriately (critical documentation is addressed by the existing PSP).

3 - Gaps: Not all confidential information is stored in secure facilities. The disposal process for confidential information is not consistently applied. Means of disposal meets bare requirements. Disposal facility is poorly secured.

4 - None/WIP: The means of disposal is inappropriate (single-cut shredder, not burn bags or multi-cut shredders) and shredder location is unsecured.

3.1	Accountability	Quality 1=Best Practice 2=Meets Reqs 3=Deficient 4=Does Not Meet Reqs Blank = Not Applicable	Execution 1=Fully 2=Critical Areas 3=Minimal/Gaps 4=None/WIP Blank = Not Applicable	Justification
3.1.4	Are procedures in place for the proper disposal of confidential information?	1	4	Agency has all the appropriate categorization, disposal and storage policies defined/ Agency has not implemented procedures (unsecured storage, single cut shredders, etc.)

Office of Information Technology Services

Scoring Guidelines - Example 2

- Quality Scoring
  - –Question: Has appropriate technology been deployed to control network access (e.g. Firewalls, VPNs, Radius, etc)?
  - –Response Details:
    - **Quality Score of:**

      1 - Best Practice: Access controls are flexible and robust enough to address all areas of existing access methods. Appropriate technologies have been identified for each access method.

      2 - Meets Requirement: Existing access methods have defined controls. Appropriate technologies have been identified.

      3 - Deficient: Select access methods have defined controls (e.g., modems are not permitted access, but are still installed). Access control technologies are outdated or at a low level of patch.

      4 - Does Not Meet Requirements: Controls PSPs are too vague for utility. Known, compromised technologies are in use. Inappropriate technologies in use.

7.3	Network Access	Quality	Execution	Justification
7.3.6	Has appropriate technology been deployed to control network access (e.g. Firewalls, VPNs, Radius, etc)?	2		

Office of Information Technology Services

Scoring Guidelines - Example 2 (Cont.)

- Execution Scoring
  - –Question: Has appropriate technology been deployed to control network access (e.g. Firewalls, VPNs, Radius, etc)?
  - –Response Details:
    - **Execution Score of:**

      1 - Fully: All access control policies, standards and procedures (PSPs) have been implemented. All access media have appropriate protection.

      2 - Critical Areas: Only critical access media have modern, encompassing technologies deployed. PSPs are adhered to for critical systems only.

      3 - Gaps: Effective technologies are in place, but not consistently across both access media. PSPs are adhered to based on personal initiative.

      4 - None/WIP: Technologies are absent to a degree that violates an effective access control.

7.3	Network Access	Quality	Execution	Justification
7.3.6	Has appropriate technology been deployed to control network access (e.g. Firewalls, VPNs, Radius, etc)?	2	4	PSPs address existing access media channels and identify appropriate technologies/technologies have yet to be addressed, even thought the Agency is in process and has an ongoing RFP process

Office of Information Technology Services

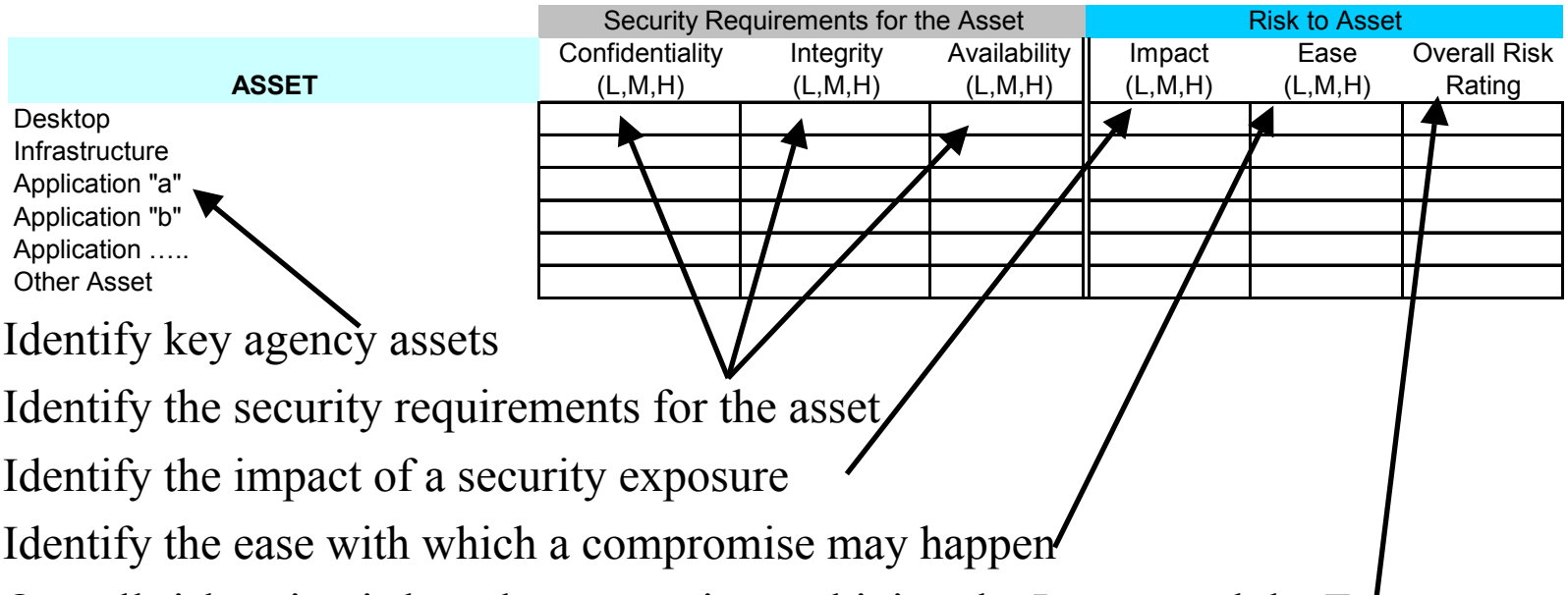
Vendor Assigned Score

- Vendor Score vs. Quality and Execution Scores
  - Vendors score each question for Quality and Execution
  - Questions in a section (and a category) roll-up to an averaged Quality/Execution score - **calculated** score
  - Based on question relevance to an Agency, vendor experience, etc., a vendor may determine that the arithmetic score does not adequately reflect the Agency's true security status
    - For each section and category, a vendor must indicate, in the Vendor Score, its own assessment of Quality and Execution.
    - The score may be similar or divergent from the arithmetic score. If divergent, a rationale must be supplied in the comments area at the bottom of the form.

Office of Information Technology Services

Executive Risk Assessment

- The purpose of Executive Risk Assessment is to identify the most critical systems/services of agency risk or exposure
- This is different from the security assessment, because the security assessment evaluates compliance to PSPs
- The risk assessment evaluates the danger and likelihood of a security exposure.



- Identify key agency assets
- Identify the security requirements for the asset
- Identify the impact of a security exposure
- Identify the ease with which a compromise may happen
- Overall risk rating is based on a matrix combining the Impact and the Ease score

Office of Information Technology Services

Security Assessment Findings Overview Guidelines

- Three to six page "executive summary"
  - More complex agency assessments may need additional pages
- Express findings in lay-terms to the extent practical
- Focus on identifying key areas of risk
- Format:
  - Executive Summary of Assessment
  - Key Findings and Analysis
    - Strengths, Weaknesses and Concerns
  - Issues and Recommendations
    - By ISO 17799 category

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Documents Overview

- *Requirements Document* - overview of project goals, assessment process, and roles and responsibilities
- *Agency Preparation Guide (Communication Package)* – provides more detailed assessment preparation guidance to agencies
- *Agency Assessment Tool*
- *Project Management Tools*
- *Project Work Break-down Structure (WBS)*
- *Agency Kick Off Meeting Presentation*

Project Management and Reporting Tools

Agency Preparation Tool Set

- *File: NC Agency Prep Tools_pv1*
  - Agency Contact Information List
  - Agency Documentation List
  - Agency Interview Schedule
  - Agency Interview Schedule Example

Vendor PM Tool Set

- *File : NC Agency PM Tools_pv1*
  - Report Cover Sheet
  - Key Findings Summary
  - Open Task Report (OTR)
  - Project Issues Log
  - Project Performance Dashboard
  - Agency Documentation List
  - Vendor Team Contact Information List
  - Vendor Time Sheet
  - Agency Preparation Tools

Please Note Naming Convention: NC AgencyAbbreviation ToolName_MMDD
(e.g. NC DOT PM Tools_1013)

Office of Information Technology Services

Agency Contact Information List

- Purpose: Capture key agency POC information
- Completed by: Agency

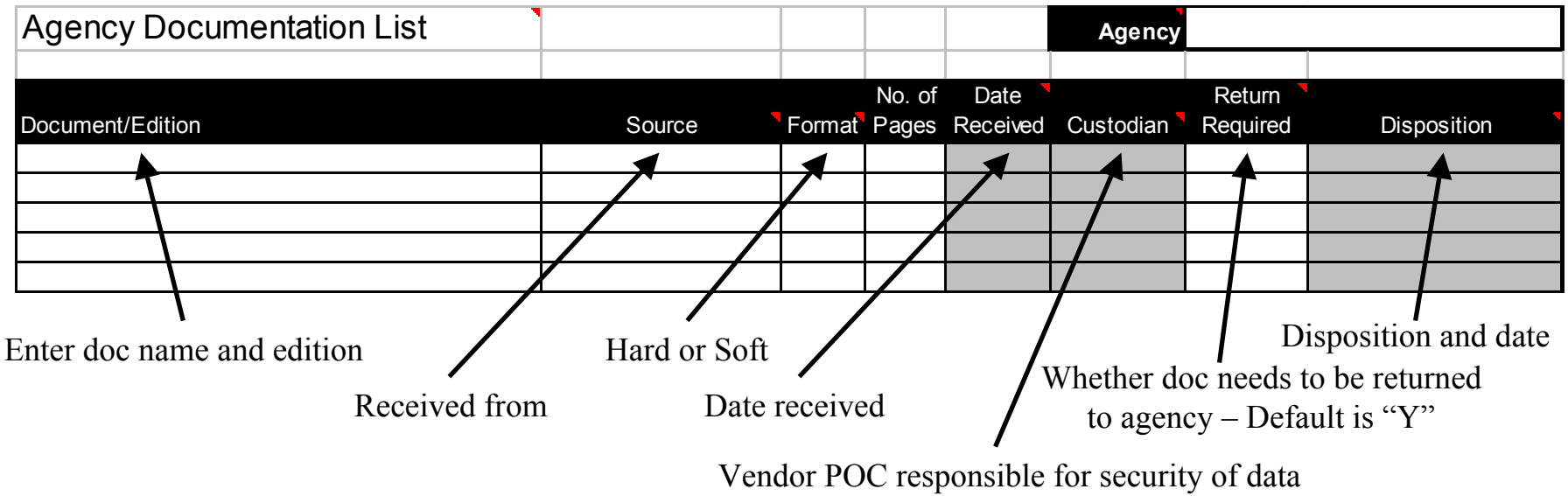
Agency Contact Information List				Agency	
	Role/Area of Focus	Name	Title	Phone #	E-mail Address
	Assessment Liaison				
	Assessment Coordinator				
1	**Security Policy**				
2	**Organizational Security**				
3	**Assest Classification & Control**				
4	**Personnel**				
5	**Physical Security**				
6	**Operations**				
7	**Access Control**				
8	**Applications**				
9	**Business Impact - Continuity**				
10	**Compliance**				

- Vendor shall add the Agency Contact Information List as completed by the Agency to the PM Tools workbook

Office of Information Technology Services

Agency Documentation List

- Purpose: Memorialize and track disposition of all documentation provided by the agency to the vendor
- Completed by: Agency Updated by: Vendor



- Vendor must keep this list up-to-date and must diligently comply with documentation disposition requirements. Failure to do so may result in contract termination.

Office of Information Technology Services

Agency Interview Schedule

- Purpose: Identify and schedule all agency interviews
- Completed by: Agency Updated by: Vendor

Agency Interview Schedule			Agency	
			Date	
Time	Interviewee(s)	Title(s)	Phone # (s)	Location

- Agencies have been asked to use the provided template or to use a commonly available tool that captures the same information
- The vendor shall be responsible for updating and maintaining the Interview Schedule after the completion of the PMO/Vendor Pre-Assessment Meeting. Vendors must verify interviews with interviewees in advance.

Office of Information Technology Services

Agency PM Tools Report Cover Sheet

- Purpose: Cover Sheet
- Completed by: Vendor

Enter Agency Name

Enter Vendor Name and Point-of-Contact (POC)

Enter Date of Report

State of North Carolina

Information Resource Management Commission

Statewide Security Assessment Project

Weekly Vendor Project Status Report

Agency: Dept of Transportation

Vendor: Assessments R' Us

Vendor POC: I.M. Pseudonym

Report Date: October 20, 2003

- Please remember to keep the report date current

Office of Information Technology Services

Project Performance Dashboard

- Purpose: Report and track vendor performance against budget and schedule
- Completed by: Vendor

Project Performance Dashboard		Agency	
Performance Against Overall Assessment Project Plan			
Planned Start Date	13-Oct		**Variance**
Actual Start Date	13-Oct	0	days
Planned Completion Date	1-Dec	0	days
Estimated Completion Date	1-Dec		
Performance Against Project Plan			
Project Budget	34	($K)	
Budgeted Cost of Work Scheduled (BCWS)	5	($K planned)	
Budgeted Cost of Work Performed (BCWP)	4	($K earned value)	
Actual Cost of Work Performed (ACWP)	2	($K expended)	
Percent of Work Complete	2%		
Cost Variance	**2**	**$K under budget**	
Schedule Variance	**-1**	**$K behind schedule**	
Notes/Comments			

Enter dates

Enter project budget ($K)

Enter BCWS ($K)
(work planned to be completed as of report date)

Enter BCWP ($K)
(earned value)

Enter ACWP ($K)
(budget expended as of report date)

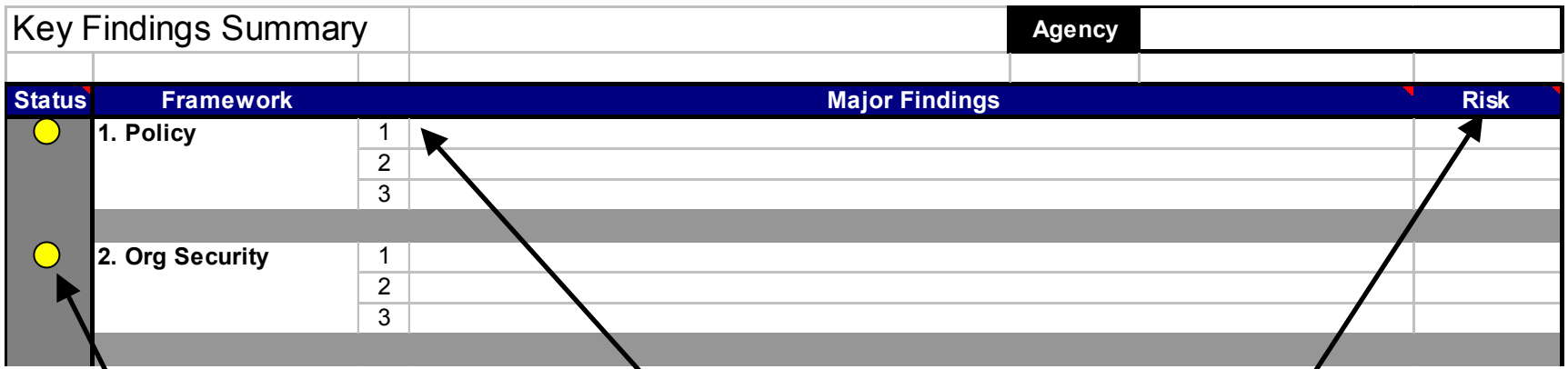
Enter any applicable comments or notes

- Helpful hint – comments boxes used throughout tools provide reminders and guidelines.

Office of Information Technology Services

Key Findings Summary

- Purpose: Report salient preliminary findings and associated security risk
- Completed by: Vendor



Change "stoplight" color to indicate holistic view of agency security posture

Identify top three findings/issues per category – provide cogent description of problem and its implications

Identify overall risk associated with finding (High/Medium/Low)

- This form provides a means to identify systemic and agency-specific issues early and facilities feedback to vendors if focus of assessment efforts seems to be off-center.

Office of Information Technology Services

Open Task Report (OTR)

- Purpose: Tracks assignments, dates and status on a by-task basis
- Completed by: Vendor

Task Number from vendor WBS

Task description of open and pending tasks

ID by initials or first name is acceptable

Task dates – due dates are established and then frozen – do not slide due dates back to cover schedule slippage

Brief status description

- Completed tasks should be noted and maintained on the OTR for one reporting cycle (one week) after which they can be removed.

Office of Information Technology Services

Project Issues Log

- Purpose: Captures and tracks project issues associated with managing project work
- Completed by: Vendor

- Simply documenting an issue in the log does not constitute proper notification. The PMO, agency, or other affected party should be notified immediately.

Office of Information Technology Services

Vendor Team Contact Information List

- Purpose: Records contact information for vendor staff
- Completed by: Vendor

Vendor Team Contact Information List			Agency	
Role	**Name**	**Title**	**Phone Number**	**E-mail Address**
Vendor Engagement Manager			O.	
			C.	
Vendor Project Manager/POC			O.	
			C.	
			F.	
Vendor Project Team Members			O.	
			C.	
			O.	
			C.	

- Please note – the PMO will typically only interface with a single vendor point-of-contact. Additional information is for security and emergency purposes only.

Office of Information Technology Services

Vendor Time Sheet

- Purpose: Records vendor work effort for project tracking and payment purposes
- Completed by: Vendor

Vendor Time Sheet

Agency Assessed: PO #:

Vendor:

Vendor Point of Contact:

	Summary Statistics		
	TTD	Cap	Remaining
Hours	0		0
Cost	$ -	$ -	$ -

Name	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	TTD
									0
									0
									0
									0
									0
									0
									0
									0
									0
									0
Total Hours For Week:	0	0	0	0	0	0	0	0	0
Blended Rate:		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Weekly Cost:	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Vendor POC Initial:									
Date:									

Final Submital Vendor Signature/Date

I hereby certify that the above is true and accurate to the best of my knowledge.

Fill-in Hours Cap and Blended Hourly Rate in addition to other fields

- Vendors cannot be paid without an accurate, up-to-date, and initialed time sheet
- Please note hours cap - the PMO cannot authorize additional funding in case of an overrun.

Office of Information Technology Services

Task Effort Estimate

Activities per Agency	Task Duration (calendar hours) Type 1	Type 2	Type 3
Step 7. Project Status Reporting			
7.1 Prepare Weekly Update Reports	3	3	3
7.1 Conduct Weekly PMO Status Meeting	2	2	2
Step 8. Prepare for Agency Assessment			
8.1 Conduct Pre-Assessment Meeting	1	1	1
8.2 Review Agency Materials	4	8	16
8.3 Finalize Interview Schedule and Plan	2	2	2
Step 9. Conduct Agency Assessment			
Task 9.1. Collect Information			
9.1.1 Conduct Assessment Kickoff Meeting	1	1	1
9.1.2 Conduct Assessment Interviews	16	24	40
9.1.3 Collect and Review Documentation	22	40	50
9.1.4 Conduct Compliance Review	4	8	16
9.1.5 Develop Preliminary Findings	8	12	16
Task 9.2. Analyze Data and Prepare Reports			
9.2.1 Complete Assessment Documentation	16	28	32
9.2.2 Develop Findings Summary	4	4	4
9.2.3 Conduct PMO Debrief / Revisions	14	14	14
Step 10. Assessment Closeout			
10.2 Schedule Agency Debrief	1	1	1
10.3 Conduct Agency Debrief	2	2	2
Total duration per category (calendar hours)	100	150	200
Size of Team (persons per task*)	2	2	2
Person-Hours to Complete Assessment	200	300	400
(* vendors may choose to use more staff; hours are fixed)			

Office of Information Technology Services

Schedule

Activity/Deadline	Date	Notes
Vendor Bid Responses Due	Sept. 3	Completed
Vendor Selection Complete	Sept. 15	Completed
Agency Project Overview Briefing (Session 1)	Sept. 25	1:30pm-3:30pm Department of Cultural Resources Auditorium
Agency Project Overview Briefing (Session 2)	Sept. 30	2pm-4pm Department of Cultural Resources Auditorium
Vendor Assessment Training	Oct. 8	1pm-5pm Department of Cultural Resources Auditorium
Security Assessment Report Due	May 4	

Assessment Activity	Start Date	End Date	Notes
Agency Assessment - Group 1	Oct. 13	Dec. 4	At agency location
Agency Assessment - Group 2	Dec. 2	Feb. 3	At agency location
Agency Assessment - Group 3A	Jan. 12	March 24	At agency location
Agency Assessment - Group 3B	Jan. 28	March 24	At agency location

Office of Information Technology Services

Agency Assessment Tracks
Group 1

Agency	Start	End
Secretary of State	10/13/03	12/1/03
Labor	10/13/03	12/1/03
Auditor	10/13/03	12/1/03
Administration	10/13/03	12/1/03
Environment & Natural Resources	10/13/03	12/1/03
ITS	10/13/03	12/1/03
Health & Human Services	10/13/03	12/4/03
Dept of Transportation	10/13/03	12/4/03
Corrections	10/13/03	12/4/03

Office of Information Technology Services

Agency Assessment Tracks
Group 2

Group 2		
Agency	**Start**	**End**
Public Instruction	12/2/03	1/27/04
Dept of Insurance	12/2/03	1/27/04
Community College System	12/2/03	1/27/04
Dept of Juvenile Justice	12/2/03	2/3/04
Dept of Crime Control	12/2/03	2/3/04
Department of Commerce	12/2/03	2/3/04
Department of Agriculture	12/2/03	2/3/04

Office of Information Technology Services

Agency Assessment Tracks
Group 3

Group 3		
Agency	**Start**	**End**
Office of the Governor	2/4/04	3/17/04
Office of the Lt. Governor	2/4/04	3/17/04
Office of State Personnel	1/12/04	2/23/04
Office of State Budget and Mgmt	2/4/04	3/17/04
Department of Cultural Resources	2/4/04	3/17/04
Office of State Controller	1/12/04	3/1/04
Employment Security Commission	1/28/04	3/17/04
Dept of Justice	1/28/04	3/17/04
Department of State Treasurer	2/4/04	3/24/04
Department of Revenue	1/12/04	3/1/04

Office of Information Technology Services

Agenda

Topic	Presenter	Time (mins)
Welcome/Introductions /Comments	Ann Garrett, Chief Information Security Officer	15
State Policies	Ann Garrett, Chief Information Security Officer	15
Project Overview	Lance Westerlund, PMP, Gartner	45
Break		15
Assessment Tool Familiarization	Daniel Saroff, Gartner	30
Project Management Tools/Schedule	Lance Westerlund, Gartner	45
Questions & Answers/Next Steps	Lance Westerlund, Gartner	30

Next Steps

Attend Pre-assessment Meeting
Review Agency Materials
Verify/Coordinate Agency Interview Schedule
Lead the Agency Kick-off Meeting
Being Assessment Data Collection and Diligence

Questions?

Office of Information Technology Services

PMO Contact

Charles “Chip” Moore
(919) 875-3792
security.pmo@ncmail.net

All hard copy documentation must be sent to the following mailbox:
Charles Moore, ITS
P.O. Box 17209
Raleigh, NC 27619